The Domain Controller (DC) is the server that is running the Active Directory Domain Services.

Primary/backup vs Multimaster domain controllers

There are often at least two domain controllers in a forest. In Windows NT t Before Active Directory was introduced with Windows 2000 the Domain Controllers were structured in a master-worker relationship where you had one DC functioning as the Primary DC and all other DCs were backup domain controllers. Back then it was only possible for the Primary DC to make domain changes - such as adding new users. The changes were then replicated to the backup domain controllers. This structure was deprecated when Active Directory was introduced in Windows 2000. Instead the architecure is based on a multimaster replication. That means that any writable DC can make changes, like adding a user, and that change will then be replicated to the other domain controllers.

Flexible Single Master Operation (FSMO) / Single Master Operation / Operations Master

So Domain Controllers in modern Active Directory use a multi-master structure, they replicate between each other all the time. However, there are certain tasks that are not so well suited for multi-master replication. These activities are called FSMO Roles, and there are five roles.

Two on the forest level, and three on the domain level.

FSMO Roles

- Schema Master - Forest - Schema updates are processed on this DC.
- Domain Naming Master - Forst - Controls changes to the forest, such as addition and removal of domains.
- PDC Emulator - Domain - See below
- RID Master - Domain - Relative Identifier (RID) Master issues pools of unique identifiers to domain controllers for them to use when new objects are created.
- Infrastructure Master - Domain - Maintains references to objects in other domains; for example, users in another domain who are member of a group in the current domain.

The first DC that is create in a in a forest performs all these roles. When a new domain is created the three domain-level services are hosted on the domain controller in that domain.

Primary Domain Controller (PDC) Service

Originally the Emulated Primary Domain Controller (PDC) service was created to be backwards compatible with pre-Window 2000 systems. On one DC there is a service running which is called `PDC`. You can find out which Domain Controller that is emulating the role of Primary DC with the following command:

```
get-addomaincontroller -discover -service PrimaryDC
```

The PDC Emulator have some new responsibilities.

- Responsible for changing passwords and monitoring user locks for password errors.
- The Group Policy Editor by default connects to the PDC Emulator server and all changes to the GPO in reality occur on it.
- By default, the PDC Emulator is the time server for the clients in the domain.
- Changes to the Distributed File System (DFS) namespace are made on the domain controller with the PDC Emulator role.
- The process of increasing the domain or forest functional level is performed on the Primary Domain Controller Emulator.
- Active Directory has so-called Well Known Security principals. Examples are the Everyone, Authenticated Users, System, Self, and Creator Owner. They are all managed by a domain controller with the PDC Emulator role.

Writable DC vs Read-only DC (RODC)

There are two types of Domain controllers **Writable DC** and a **Read-only DC**

Writable DC This is just the standard Domain Controller.

Read-only DC (RODC)

Forest Function Level

References

https://adsecurity.org/?p=3592